539164

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年7 月1 日 (01.07.2004)

PCT

(10) 国際公開番号
WO 2004/055680 A1

(51) 国際特許分類[7]: G06F 12/14, G06K 19/073

(21) 国際出願番号: PCT/JP2003/016000

(22) 国際出願日: 2003 年12 月12 日 (12.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-363597
2002 年12 月16 日 (16.12.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 高木 佳彦 (TAKAGI,Yoshihiko) [JP/JP]; 〒144-0046 東京都 大田区 東六郷２−２０−５−５０６ Tokyo (JP). 中西 良明 (NAKANISHI,Yoshiaki) [JP/JP]; 〒166-0014 東京都 杉並区 松ノ木２−４−１０−３０５ Tokyo (JP). 佐々木 理 (SASAKI,Osamu) [JP/JP]; 〒144-0046 東京都 大田区 東六郷２−２０−５−６２０ Tokyo (JP). 菊地 隆文 (KIKUCHI,Takafumi) [JP/JP]; 〒144-0046 東京都 大田区 東六郷２−２０−５−７１８ Tokyo (JP).

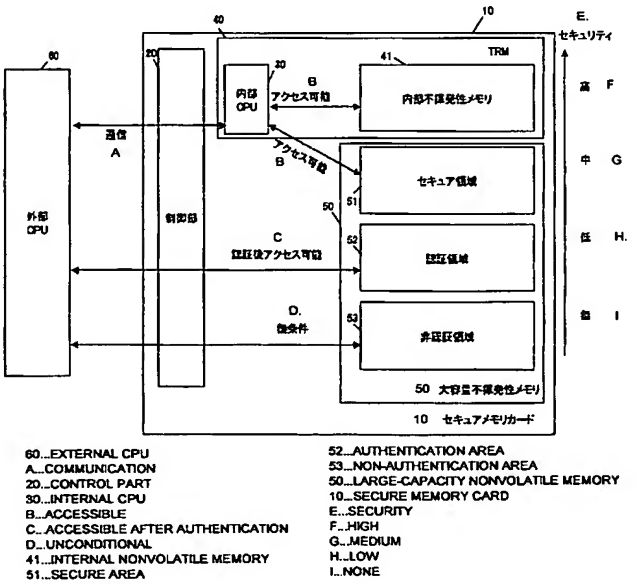
(74) 代理人: 小栗 昌平, 外 (OGURI,Shohei et al.); 〒107-6013 東京都 港区 赤坂一丁目１２番３２号 アーク森ビル１３階 栄光特許事務所 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

[続葉有]

(54) Title: MEMORY DEVICE AND ELECTRONIC DEVICE USING THE SAME

(54) 発明の名称: メモリデバイスとそれを使用する電子機器



(57) Abstract: A memory card having a large storage capacity and a memory area that has an equivalent level of security to IC cards. A semiconductor memory card (10) attachable to and removable from an electronic device has a non-tamper-resistant first memory (50) comprising ordinary areas (52,53) that are accessible from the electronic device and a secure area (51) that is not directly accessible from the electronic device, and also has a tamper-resistant second memory (41) that is not directly accessible from the electronic device. The semiconductor memory card (10) is so configured that the secure area (51) of the first memory (50) can be accessed only via a secure control part (30) that manages the access to the second memory (41). The secure area (51) cannot be directly accessed from any external device and hence exhibits a higher security level than an authentication area (52). Moreover, since the secure area (51) is provided in the non-tamper-resistant memory (50), it can have a large storage capacity.

[続葉有]

WO 2004/055680 A1

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

(57) 要約: 本発明は、記憶容量が大きく、且つ、ICカードと同等のセキュリティレベルを有するメモリ領域を備えたメモリカードを提供することを目的とする。電子機器に着脱可能な半導体メモリカード10に、電子機器からアクセスすることが可能な通常領域52,53と、電子機器から直接アクセスすることができないセキュア領域51とを有する非耐タンパー性の第1のメモリ50と、電子機器から直接アクセスすることができない耐タンパー性の第2のメモリ41とを設け、第1のメモナ50のセキュア領域51へのアクセスが、第2のメモリ41へのアクセスを管理するセキュア制御部30を介してのみ可能であるように構成している。このセキュア領域51は、外部機器が直接アクセスできないため、認証領域52よりもセキュリティレベルが高い。また、このセキュア領域51は、非耐タンパー性のメモリ50に設けられるため、記憶容量を大きく取ることができる。

明細書

メモリデバイスとそれを使用する電子機器

＜技術分野＞

本発明は、半導体メモリカードなどのメモリデバイスと、このメモリデバイスへのデータの書き込み／読み出しを行う電子機器に関し、特に、セキュリティレベルが高く、大きい記憶容量を持つ記憶媒体の実現を図るものである。

＜背景技術＞

不揮発性の半導体メモリを記憶媒体として具備する半導体メモリカード（以下、「メモリカード」と言う）は、ＤＶＤなどのディスク状記憶媒体に比べて、記憶容量は小さいが、大きな機構部を必要とせず、小型で取り扱いが容易で、耐震性にも優れているため、携帯用に好適な記憶媒体として、最近、その利用範囲が拡大している。

メモリカードには、ＣＰＵ（マイコン）を内蔵したものとＣＰＵを内蔵しないものとがある。ＣＰＵを内蔵したメモリカードにおけるＣＰＵの働きは、外部機器から要求される、不揮発性メモリの読み出し・書き込み処理である。

また、メモリカードの不揮発性メモリにセキュア領域を設けて、セキュリティレベルを高める工夫も行われている。下記特許文献１には、不揮発性メモリ内に、認証に成功した外部機器のみがアクセスできる認証領域と、外部機器のいずれもがアクセスできる非認証領域とを設けたメモリカードが記載されている。このメモリカードを用いて、暗号化した音楽コンテンツを非認証領域に格納し、それを復号する復号鍵を認証領域に格納することにより、コンテンツの著作権を守ることが可能になる。

このようなメモリカードにおけるＣＰＵの働きは、読み出し・書き込み処理に加えて、外部機器による認証領域へのアクセスを許可するための外部機器の認証処理がある。

いずれにしろ、メモリカードにおけるＣＰＵの働きは、メモリの読み書き及びそれに付随したものに限定され、メモリに記録されたデータの制御は外部機器によって行われる。

一方、同様にＣＰＵを内蔵するＩＣカードは、耐タンパー性のモジュール内にＣＰＵとともにメモリ領域を有している。耐タンパーゆえ、外部機器は、このメモリ領域に直接アクセスすることができない。そのため、ＩＣカードは、複製や偽造に対して高い守秘性があり、高いセキュリティレベルが要求されるデジタルキャッシュのサービス等で利用されている。

ＩＣカードにおけるＣＰＵの働きは、メモリの読み出し・書き込みのみならず、外部から入力されたデータの暗号化、署名生成、署名検証、入力された暗証番号照合など、多岐に渡る。また、ＩＣカードのメモリに記録されたデータの制御はＩＣカード内部ＣＰＵによって行われる。

このように、ＩＣカードのＣＰＵは、従来のメモリカードに内蔵されるＣＰＵに比べて、多機能かつ高セキュリティである。

［特許文献１］

特開２００１－１４４４１号公報

しかし、ＩＣカードは、蓄積できる情報容量が限られており、デジタルキャッシュのサービスの多様化と共に、蓄積容量の拡大がサービス業者等から求められている。例えば、デジタルキャッシュの２重引き落とし等のトラブルを回避する目的で、電子レシートや取引ログを記録するサービスを実施しようとすると、累積する電子レシート等を蓄積するために、従来のＩＣカードの容量に比べて、大きな情報容量の確保が必要になる。

一方、前記特許文献１に記載されているメモリカードは、認証領域が可変に設定できるため、ある程度大きな情報容量を持たせることが可能である。しかし、この認証領域は、外部機器が直接制御可能な領域であるため、ＩＣカードに比べてセキュリティレベルは低い。

＜発明の開示＞

本発明は、こうした従来の問題点を解決するものであり、記憶容量が大きく、且つ、ＩＣカードと同等のセキュリティレベルを有するメモリ領域を備えたメモリデバイスを提供し、また、そのメモリデバイスを使用する電子機器を提供することを目的としている。

そこで、本発明では、電子機器に固定的にまたは着脱可能に接続されるメモリデバイスに、電子機器からアクセスすることが可能な通常領域と、電子機器から直接アクセスすることができないセキュア領域とを有する非耐タンパー性の第１のメモリと、電子機器から直接アクセスすることができない耐タンパー性の第２のメモリとを設け、第１のメモリのセキュア領域へのアクセスが、第２のメモリへのアクセスを管理するセキュア制御部を介してのみ可能であるように構成している。

このセキュア領域は、外部機器が直接アクセスできないため、従来の認証領域よりもセキュリティレベルが高い。また、このセキュア領域は、非耐タンパー性のメモリに設けているため、低コストで大きい記憶容量を取ることができる。

また、本発明では、メモリ領域として第１領域、第２領域及び第３領域を有するメモリデバイスに対してアクセスを行う電子機器が、メモリデバイスへのアクセス要求を受けたときに、メモリデバイスの非耐タンパー性のメモリ領域である第１領域には、メモリデバイスへのアクセスを制御するメモリデバイスの全体制御部を介してアクセスを行い、第１領域以外の非耐タンパー性のメモリ領域である第２領域には、全体制御部と、第２領域及び第３領域へのアクセスを制御するメモリデバイスのセキュア制御部とを介して、セキュア制御部との認証を経た後、アクセスを行い、また、メモリデバイスの耐タンパー性のメモリ領域である第３領域には、全体制御部及びセキュア制御部を介して、セキュア制御部との認証を経た後、アクセスを行うように構成している。

この電子機器は、この半導体メモリカード等のメモリデバイスを活用して、多様なサービスの実現を図ることができる。

＜図面の簡単な説明＞

図１は、本発明の実施形態におけるセキュアメモリカードの概念図；

図２は、本発明の実施形態におけるセキュアメモリカードの構成を示すブロック図；

図３は、本発明の実施形態におけるセキュアメモリカードを使用するシステムの概念図；

図４は、本発明の実施形態におけるＲ／Ｗ装置の構成を示すブロック図；

図５は、本発明の実施形態におけるセキュアメモリカードの書き込み手順を示すシーケンス；

図６は、本発明の実施形態におけるセキュアメモリカードの書き込み手順の続きを示すシーケンス；

図７は、本発明の実施形態におけるセキュアメモリカードの他の書き込み手順を示すシーケンス；

図８は、本発明の実施形態におけるセキュアメモリカードの大容量不揮発性メモリの構造を示す図；

図９は、本発明の実施形態における論理－物理アドレス変換テーブルを示す図；

図１０は、本発明の実施形態における論理－物理アドレス変換テーブルの他の例を示す図；

図１１は、本発明の実施形態におけるセキュアメモリカードの大容量不揮発性メモリの異なる構造を示す図；

図１２は、本発明の実施形態における論理－物理アドレス変換テーブルの異なる例を示す図である。

尚、図中の参照番号は、１０－－セキュアメモリカード；１１－－ＩＣ部；１２－－Ｉ／Ｆ部；１３－－ＩＣコマンド処理部；１４－－ファイル管理部；１５－－ＩＣ認証部；１６－－メモリ管理部；１７－－暗復号回路；１８－－内部不揮発性メモリＩ／Ｆ部；２０－－制御部；２１－－データＩ／Ｆ部；２２－－コマンドＩ／Ｆ部；２３－－制御認証部；２４－－コマンド処理部；２５－－アクセス制御部；２６－－大容量不揮発性メモリＩ／Ｆ部；４０－－ＴＲＭ；４１－－内部不揮発性メモリ；５０－－

大容量不揮発性メモリ；５１―セキュア領域；５２―認証領域；５３―非認証領域；６０―外部ＣＰＵ；６１―携帯電話；６２―ＲＯＭ；６３―ＲＡＭ；６４―液晶表示部；６５―無線通信部；６６―操作ボタン；６７―カードＩ／Ｆ部；６８―認証回路；６９―Ｒ／Ｗ装置；７０―内部バス；９１―チャージ用端末；９２―チャージサーバ；９３―決済サーバ；９４―配信サーバ；９５―ネットワーク；６２１―コマンド生成プログラム；６２２―認証鍵群
を示すものである。

＜発明を実施するための最良の形態＞

本発明の実施形態における半導体メモリカード（ここでは「セキュアメモリカード」と呼ぶことにする）は、図１の概念図に示すように、内部不揮発性メモリ４１を備える耐タンパー性モジュール（tamper resistant module：ＴＲＭ）４０と、非認証領域５３、認証領域５２及びセキュア領域５１を備える大容量不揮発性メモリ５０と、内部不揮発性メモリ４１及びセキュア領域５１に対してアクセスする内部ＣＰＵ３０と、電子機器（リード／ライト（Ｒ／Ｗ）装置）の外部ＣＰＵ６０と通信して認証処理を行い、認証した外部ＣＰＵ６０の認証領域５２へのアクセスを許可する制御部２０とを備えている。

ＴＲＭ４０の不揮発性メモリ４１は、例えば、１６バイト単位で消去・書き込みができるＥＥＰＲＯＭから成り、また、大容量不揮発性メモリ５０は、例えば、５１２バイト等のブロック単位での消去と１バイト単位での書き込みとが可能なフラッシュメモリから成る。

外部ＣＰＵ６０は、非認証領域５３に無条件でアクセスすることができ、また、認証領域５２には、制御部２０での認証を済ませた場合にアクセスすることができる。しかし、外部ＣＰＵ６０は、セキュア領域５１及び内部不揮発性メモリ４１の存在を知ることができず、これらに直接アクセスすることはできない。

セキュア領域５１及び内部不揮発性メモリ４１に対しては、内部ＣＰＵ３０だけがアクセス可能である。セキュア領域５１と内部不揮発性メモリ４１との違いは、内部不揮発性メモリ４１がＴＲＭ４０に設けられているのに対し、セキュア領域５１が、耐タンパー性を持たない大容量不揮発性メモリ５３に設けられてい

る点である。そのため、セキュア領域５１は、内部不揮発性メモリ４１に比べて大きい蓄積容量を持つことができる。その反面、セキュリティレベルは、ＴＲＭ４０に設けられた内部不揮発性メモリ４１よりも低い。この４つの領域のセキュリティレベルは、非認証領域５３が最も低く、認証領域５２、セキュア領域５１、内部不揮発性メモリ４１の順に高くなっている。

セキュアメモリカード１０の構成の詳細は後述するとして、その使用形態について説明する。

セキュアメモリカードは、例えば、図３に示す音楽配信システムなどで使用することができる。このシステムでは、セキュアメモリカード１０がＲ／Ｗ装置である携帯電話６１に装着される。また、このシステムには、ネットワーク９５を介して音楽を配信する配信サーバ９４と、決済処理を行う決済サーバ９３と、デジタルキャッシュをメモリカード１０にチャージするチャージサーバ９２と、デジタルキャッシュのチャージ用端末９１とが存在している。

携帯電話６１は、図４のブロック図に示すように、図１の外部ＣＰＵに相当するＣＰＵ６０と、認証に使用する認証鍵群６２２やコマンド生成プログラム６２１を予め記憶しているＲＯＭ６２と、ＣＰＵ６０の作業領域として使用されるＲＡＭ６３と、表示画面を構成する液晶表示部６４と、ネットワークを介して無線通信を行う無線通信部６５と、ユーザが操作する操作ボタン６６と、セキュアメモリカード１０を内部バス７０に接続するカードＩ／Ｆ部６７と、セキュアメモリカード１０との相互認証を行う認証回路６８とを備えており、これらの各部が内部バス７０で接続されている。

ユーザは、まず、セキュアメモリカード１０にデジタルキャッシュをチャージする。そのために、ユーザは、セキュアメモリカード１０をチャージ端末９１に装着し、表示された指示に従ってチャージ端末９１を操作する。このとき、チャージ端末９１は、セキュアメモリカード１０の内部ＣＰＵ３０に入金アプリケーションの起動を要求する。入金アプリケーションを起動した内部ＣＰＵ３０は、チャージ端末９１からデジタルキャッシュの入金処理要求を受けると、その要求のコマンドから、データの書き込み先を内部不揮発性メモリ４１と判断し、チャ

ージ端末９１から伝えられた金額を内部不揮発性メモリ４１に書き込む。こうして内部不揮発性メモリ４１にキャッシュ情報が蓄積される。

また、デジタルキャッシュのチャージは、セキュアメモリカード１０を装着した携帯電話６１から、チャージサーバ９２にアクセスして、オンラインで行うこともできる。

次に、ユーザは、携帯電話６１から配信サーバ９４にアクセスし、音楽コンテンツの購入を依頼する。配信サーバ９４は、音楽コンテンツの代金の決済を要求する。これを受けて携帯電話６１のＣＰＵ６０は、セキュアメモリカード１０の内部ＣＰＵ３０に決済アプリケーションの起動を要求する。決済アプリケーションを起動した内部ＣＰＵ３０は、携帯電話６１を認証した後、携帯電話６１から伝えられた支払額を内部不揮発性メモリ４１に記録されたデジタルキャッシュの残額から減算する。これを受けて配信サーバ９４は、電子レシートを携帯端末６１に送信し、携帯端末６１のＣＰＵ６０は、この電子レシートの格納要求をセキュアメモリカード１０の内部ＣＰＵ３０に送る。内部ＣＰＵ３０は、その要求のコマンドから、データの書き込み先をセキュア領域５１と判断して、電子レシートをセキュア領域５１に蓄積する。

なお、決済処理は、内部不揮発性メモリ４１に格納されたクレジット番号を決済サーバ９３に提示して、決済サーバ９３との間で行うこともできる。

決済の終了後、配信サーバ９４は、暗号化された音楽コンテンツと、その復号鍵とを携帯電話６１に送信する。携帯電話６１のＣＰＵ６０は、受信データを判断し、コンテンツの復号鍵をセキュアメモリカード１０の認証領域５２に格納し、また、暗号化されたコンテンツをセキュアメモリカード１０の非認証領域５３に格納する。

このように、このシステムでは、セキュアメモリカード１０のＴＲＭ４０の内部不揮発性メモリ４１にはキャッシュ情報が格納され、セキュア領域５１には電子レシートが、認証領域５２には復号鍵が、また、非認証領域５３には暗号化されたコンテンツがそれぞれ格納される。

図２のブロック図は、セキュアメモリカード１０の構成を示している。セキュアメモリカード１０は、大別して、制御部２０と、大容量不揮発性メモリ５０と、

図１のＴＲＭ４０に相当するＩＣ部１１とで構成される。大容量不揮発性メモリ５０は、非認証領域５３と、認証領域５２と、セキュア領域５１と、これらの領域のアドレス情報が格納されたアドレス情報管理領域５４とを有している。

制御部２０は、Ｒ／Ｗ装置６９との間でデータの授受を行うデータＩ／Ｆ部２１と、Ｒ／Ｗ装置６９との間でコマンドの授受を行うコマンドＩ／Ｆ部２２と、Ｒ／Ｗ装置６９を認証する制御認証部２３と、受け付けたコマンドを解釈してコマンドに応じた処理を行う制御コマンド処理部２４と、大容量不揮発性メモリ５０へのアクセスを制御するとともにＩＣ部１１とのデータの受け渡し窓口となるアクセス制御部２５と、大容量不揮発性メモリ５０との間でデータを受け渡す大容量不揮発性メモリＩ／Ｆ部２６とを備えている。

また、耐タンパー性のＩＣ部１１は、内部不揮発性メモリ４１と、制御部２０との間でデータやコマンドの授受を行うＩ／Ｆ部１２と、コマンドを解釈してコマンドに応じた処理を行うＩＣコマンド処理部１３と、内部不揮発性メモリ４１及びセキュア領域５１にファイル形式で格納されたデータを管理するファイル管理部１４と、Ｒ／Ｗ装置６９を認証し、認証したＲ／Ｗ装置６９に対して内部不揮発性メモリ４１及びセキュア領域５１へのデータアクセスを許可するＩＣ認証部１５と、内部不揮発性メモリ４１及びセキュア領域５１への書き込み／読み出しデータに対して内部不揮発性メモリ４１に格納された鍵を用いて暗号化／復号化を行う暗復号回路１７と、内部不揮発性メモリ４１及びセキュア領域５１の管理を行うメモリ管理部１６と、内部不揮発性メモリ４１へのデータの授受を行う内部不揮発性メモリＩ／Ｆ部１８とを備えている。特許請求の範囲で云うセキュア制御部は、ＩＣ部１１のＩＣコマンド処理部１３、ＩＣ認証部１５、暗復号化回路１７、ファイル管理部１４及びメモリ管理部１６に対応する。

制御部２０の制御コマンド処理部２４は、Ｒ／Ｗ装置６９から受信したコマンドを解釈し、そのコマンドが

・大容量不揮発性メモリ５０の認証領域５２または非認証領域５３へのアクセスを要求するものであるか、

・認証を要求するものであるか、

・ＩＣ部１１による処理を要求するものであるか

を判断し、大容量不揮発性メモリ５０の認証領域５２または非認証領域５３へのアクセスを要求しているときは、アクセス制御部２５に大容量不揮発性メモリ５０へのアクセス制御を指示し、ＩＣ部１１による処理を要求しているときは、アクセス制御部２５にＩＣ部１１へのコマンドの転送を指示し、また、認証を要求しているときは、制御認証部２３に認証処理を指示する。

認証領域５２へのアクセスは、その端末に対する制御認証部２３の認証が済んでいる場合にのみ、受け入れられる。

アクセス制御部２５は、大容量不揮発性メモリ５０へのアクセス制御に当たって、大容量不揮発性メモリ５０のアドレス情報管理領域５４に記録されたアドレス情報を参照する。端末（Ｒ／Ｗ装置６９）が大容量不揮発性メモリ５０の論理アドレスを指定してアクセスを求めて来たときは、アドレス情報管理領域５４の記録から、指定されたアドレスが大容量不揮発性メモリ５０のいずれの領域に属しているかを判断し、認証領域５２へのアクセス要求に対しては、認証済み端末に限って許可する。

また、ＩＣ部１１のＩＣコマンド処理部１３は、制御部２０から送信されたコマンドを解釈し、その処理要求が、

・内部不揮発性メモリ４１へのデータ書き込み／読み出しを要求するものであるか、

・セキュア領域５１へのデータ書き込み／読み出しを要求するものであるか、

・認証を要求するものであるか、

・その他の処理を要求するものであるか

を判断する。

ＩＣコマンド処理部１３は、コマンドがアプリケーションの起動を要求しているときには、内部にそのアプリケーションを起動する。

アプリケーションとは、Ｒ／Ｗ装置６９から受け取ったコマンドの解釈形態であり、アプリケーション起動後にＲ／Ｗ装置６９からＩＣコマンド処理部１３が受け取ったコマンドは、そのアプリケーションとＲ／Ｗ装置６９との間で取り決めた解釈がＩＣコマンド処理部１３によって行われる。

アプリケーション起動後に受け取ったコマンドが、認証を要求しているときには、ＩＣコマンド処理部１３は、ＩＣ認証部１５にＲ／Ｗ装置６９の認証処理を指示する。

また、ＩＣコマンド処理部１３は、コマンドが、内部に起動したアプリケーションとＲ／Ｗ装置６９との間で取り決めた、内部不揮発性メモリ４１へのデータの書き込み／読み出し、または、セキュア領域５１へのデータの書き込み／読み出しを要求するコマンドであるときは、ＩＣ認証部１５において認証処理が済まされているか確認する。

認証処理が済まされている場合は、その要求を許可し、その要求が書き込み求であるときは、書き込むデータを、格納先の情報を付してメモリ管理部１６に送る。

内部不揮発性メモリ４１及びセキュア領域５１を管理するメモリ管理部１６は、書き込むデータを暗復号回路１７で暗号化（このとき暗復号回路１７は、内部不揮発性メモリ４１に格納された暗号鍵を用いて暗号化を行う）した後、内部不揮発性メモリ４１に書き込むべきデータを、内部不揮発性メモリＩ／Ｆ部１８を介して、内部不揮発性メモリ４１に書き込み、書き込み位置の情報をファイル管理部１４に伝える。また、セキュア領域５１に書き込むべきデータを、大容量不揮発性メモリＩ／Ｆ部２６を介して、大容量不揮発性メモリ５０のセキュア領域５１に書き込み、書き込み位置の情報をファイル管理部１４に伝える。

ファイル管理部１４は、メモリ管理部１６から伝えられた情報を基に、内部不揮発性メモリ４１及びセキュア領域５１に格納されたファイルを管理する。

また、ＩＣコマンド処理部１３は、その要求が読み出し要求であるときは、読み出すべきデータのファイル位置をファイル管理部１４に求め、メモリ管理部１６にそのファイルの読み出しを要求する。

メモリ管理部１６は、そのファイルをメモリ管理部１６が内部不揮発性メモリ４１またはセキュア領域５１から読み出すと、暗復号回路１７でデータを復号化（このとき暗復号回路１７は、内部不揮発性メモリ４１に格納された鍵を用いて復号化を行う）して、ＩＣコマンド処理部１３に送る。

復号化されたデータは、制御部２０に送られ、データＩ／Ｆ部２１からＲ／Ｗ装置６９に送信される。

ここで、大容量不揮発性メモリ５０の非認証領域５３、認証領域５２及びセキュア領域５１、並びに内部不揮発性メモリ４１への書き込み／読み出し条件を整理すると次のようになる。

・非認証領域：無条件でアクセス可能である。非認証領域５３にアクセスするための通常コマンドでデータの書き込み／読み出しを行うことができる。

・認証領域：制御部２０の制御認証部２３との認証を済ませることが必要である。制御認証部２３が認証することによって認証領域５２の論理アドレスを用いてアクセスすることが可能となる。

・セキュア領域：ＩＣ部１１のＩＣ認証部１５（＝ＩＣ部アプリケーション）との認証を済ませることが必要である。ＩＣ部アプリケーションと端末との間で取り決めたコマンドによりデータの書き込み／読み出しが可能になる（またはＩＣ部アプリケーションの処理の一部としてデータの書き込み／読み出しが可能になる）。端末からはセキュア領域を見ることができず、端末は、セキュア領域の論理アドレスを用いてアクセスすることはできない。

・内部不揮発性メモリ：セキュア領域の書き込み／読み出し条件と全く同じである。なお、セキュア領域にアクセスするための認証と内部不揮発性メモリにアクセスするための認証とを異なるものとしてもよい。

図８は、大容量不揮発性メモリ５０の内部構造を示している。ここでは、大容量不揮発性メモリ５０の物理アドレス上の配置が、非認証領域５３は0000～(XXXX-1)、認証領域５２はXXXX～(ZZZZ-1)、セキュア領域５１はZZZZ～(YYYY)の場合を示している。セキュア領域５１と認証領域５２との境界を示す第１アドレス情報はZZZZであり、認証領域５２と非認証領域５３との境界を示す第２アドレス情報はXXXXである。また、非認証領域５３のサイズはXXXX、認証領域５２のサイズはZZZZ-XXXX、セキュア領域５１のサイズはYYYY-ZZZZ+1である。

図９は、各領域の物理アドレスと論理アドレスとの対応関係を表す「論理－物理アドレス変換テーブル」を示している。非認証領域５３の論理アドレスは

0000～(XXXX-1)であり、認証領域５２の論理アドレスは0000～(ZZZZ-XXXX-1)、セキュア領域５１の論理アドレスは0000～(YYYY-ZZZZ)である。

アドレス情報管理領域５４には、第１アドレス情報、第２アドレス情報、及び、各領域の論理－物理アドレス変換テーブルが保持されている。非認証領域５３、認証領域５２、及びセキュア領域５１のいずれについても、割り当てられた論理アドレスの境界を越えて論理アドレスを指定することはできないが、各領域の境界を移動して、各領域を拡張または縮小することはできる。

セキュア領域５１の拡張／縮小は、第１アドレス情報を変更することによって実現できる。図９の論理－物理アドレス変換テーブルでは、非認証領域５３及び認証領域５２における論理アドレスの順番を物理アドレスの順序の正順とし、セキュア領域５１における論理アドレスの順番を物理アドレスの順序の逆順としているので、認証領域５２とセキュア領域５１との境界を変更したとき、ともに論理ブロックの末尾アドレスの側だけを修正すれば足りるので、境界変更に伴うテーブルの書き換え負担が少なくなり、高速での処理が可能になる。

この境界変更の手順については後述する。

次に、このセキュアメモリカードでのデータの格納手順について説明する。

図５及び図６は、セキュアメモリカードを装着した端末から配信サーバにコンテンツ購入を依頼し、代金の決済処理を行い、その電子レシートをセキュア領域に、暗号化されたコンテンツを非認証領域に、また、コンテンツの復号鍵を認証領域に格納するまでの手順を示している。

図５に示すように、端末は配信サーバにコンテンツ購入を依頼する（１）。配信サーバは、コンテンツの代金の決済を要求する（２）。端末は、セキュアメモリカード１０のＩＣ部１１に決済アプリケーションの起動を要求するコマンドを送信する（３）。制御部２０の制御コマンド処理部２４は、このコマンドをＩＣ部に対するコマンドであると認識して、ＩＣ部１１に送信する（４）。ＩＣ部１１は、決済アプリケーションを起動してＩＣ認証部１５を立ち上げ、応答を端末に返す（５）、（６）。端末は、セキュアメモリカード１０に認証要求コマンドを送り（７）、制御部２０の制御コマンド処理部２４は、このコマンドをＩＣ部に対するコマンドであると認識して、ＩＣ部１１に送信する（８）。ＩＣ認証部

１５は、端末（または配信サーバ）を認証し、認証結果を応答する（９）、（１０）。認証が済んだ端末は、セキュアメモリカード１０に支払額を示し、決済要求のコマンドを送信する（１１）。制御部２０の制御コマンド処理部２４は、このコマンドをＩＣ部に対するコマンドであると認識して、ＩＣ部１１に送信する（１２）。ＩＣ認証部１５は、「決済要求」というコマンドにより内部不揮発性メモリ４１に書き込むデータであることを判断し、内部不揮発性メモリ４１に記録された残高を、支払額を減算した額に書き換える処理を行い、処理終了を応答する（１３）、（１４）（なお、端末が（９）の認証を済ませていない状態での決済要求は拒否される）。

端末は、配信サーバに応答を返す（１５）。配信サーバは電子レシートを端末に送信する（１６）。端末は、セキュアメモリカード１０に電子レシートの格納要求コマンドを送信する（１７）。制御部２０の制御コマンド処理部２４は、このコマンドをＩＣ部に対するコマンドであると認識して、ＩＣ部１１に送信する。ＩＣ認証部１５は、「電子レシート格納要求」というコマンドによりセキュア領域５１に格納すべきデータであると判断し、電子レシートを暗復号回路１７で暗号化した後、セキュア領域５１に格納する（１８）（なお、端末が（９）の認証を済ませていない状態での電子レシート格納要求は拒否される）。

なお、ＩＣ認証部１５による（９）の認証は、「決済要求」を許可するための認証と、「電子レシート格納要求」を許可するための認証とを別に行うようにしてもよい（つまり、異なる鍵を用いて認証することを必要とする、としてもよい）。

図６に示すように、電子レシートの格納済みの応答がＩＣ部１１から端末に送られると（１９）（２０）、端末は配信サーバにコンテンツの送信を要求する（２１）。配信サーバは、暗号化したコンテンツと、それを復号するコンテンツ鍵とを端末に送信する（２２）。端末は、配信サーバから受け取ったデータに、認証領域５２に書き込むべきコンテンツ鍵が含まれることを判断し、セキュアメモリカード１０の制御部２０に対して認証を要求する（２３）。制御部２０の制御コマンド処理部２４は、このコマンドを解釈して、端末の認証を制御認証部２３で行わせて、認証結果を応答する（２４）。端末は、認証領域５２へのコンテ

ンツ鍵の書き込み要求を出す（２５）。制御部２０のアクセス制御部２５は、端末の認証が済んでいるため、認証領域５２へのアクセスを許可し、認証領域５２にコンテンツ鍵が書き込まれる。書き込み終了の応答があると（２６）、端末は、暗号化されたコンテンツを非認証領域５３へ書き込むべきことを判断し、セキュアメモリカード１０に非認証領域５３へのコンテンツの書き込みを要求する（２７）。暗号化されたコンテンツが非認証領域５３に書き込まれ、その応答が端末に返ると（２８）、端末は配信サーバに完了通知を送信する（２９）。

こうして、電子レシートが暗号化してセキュア領域５１に、コンテンツ鍵が認証領域５２に、暗号化されたコンテンツが非認証領域５３に、それぞれ書き込まれる。

なお、図５の手順中、内部不揮発性メモリ４１に記録された残高を、支払額を減算した額に書き換えたとき（１３）、図７に示すように、その支払額をセキュア領域５１に書き込むようにしても良い（１３’）。こうすることで決済ログをセキュア領域５１に記録することができる。

また、決済アプリケーションによる認証（３）を行う前、または後に、利用者を確認するための暗証番号照合を行うようにしてもよい。

次に、大容量不揮発性メモリ５０における各領域間の境界変更の手順について説明する。ここでは、図８の第１アドレス情報を変更してセキュア領域５１を拡張または縮小する場合を示す。

この境界変更は、セキュアメモリカード１０を装着した端末からの要求で行われる。

（１）端末は、セキュアメモリカード１０に対して、境界変更アプリケーションの起動を要求し、このアプリケーションを起動したセキュアメモリカード１０のＩＣ部１１は、ＩＣコマンド処理部１３及びＩＣ認証部１５を立ち上げる。端末は、ＩＣ部１１に対して認証を要求し、ＩＣ認証部１５は、端末を認証する。なお、この認証は、内部不揮発性メモリ４１やセキュア領域５１へのアクセスに要する認証とは別の認証とし、一部の特定端末のみがセキュア領域５１の拡張／縮小を行うことができるようにしても良い。

（2）認証を受けた端末は、ＩＣ部アプリケーション（ＩＣコマンド処理部１３）に対して変更後の第１アドレス情報（新たなZZZZ）を通知する。

（3）ＩＣコマンド処理部１３は、メモリ管理部１６に新たなZZZZを伝えてセキュア領域５１の境界変更を指示する。メモリ管理部１６は、ZZZZの値に対応するようにセキュア領域５１と認証領域５２との論理ー物理アドレス変換テーブルを修正し、アドレス情報管理領域５４に、新たなZZZZの値と、修正した論理ー物理アドレス変換テーブルとを格納する。このとき、図９のセキュア領域及び認証領域のテーブル上で、共に論理ブロックの末尾アドレスの側だけが修正される。

（4）メモリ管理部１６は、セキュア領域５１を拡張した場合には、新たにセキュア領域となった部分のデータを消去し、セキュア領域５１を縮小した場合には、新たに認証領域５２となった部分のデータを消去する。このとき、セキュア領域、及び／または、認証領域のすべてのデータを消去してもよい。

（5）ＩＣコマンド処理部１３は、端末に境界変更完了を通知する。

また、このとき、ＩＣ部の要求に基づいて、セキュアメモリカード１０の制御部２０が、境界変更の処理を行うようにしてもよい。この場合の手順は次のようになる。

（1）前記（1）と同様に、端末がＩＣ認証部１５の認証を受ける。

（1’）端末は、セキュアメモリカード１０の制御部２０に対して認証を要求し、制御コマンド処理部２４の指示により、制御認証部２３が認証領域のサイズ変更を許可するための認証を行う。

（2）前記（2）と同様に、端末が、ＩＣコマンド処理部１３に対して変更後の第１アドレス情報（新たなZZZZ）を通知する。

（3）ＩＣコマンド処理部１３は、アクセス制御部２５を経由して、制御部コマンド処理部２４に境界アドレス変更を要求する。

（3’）制御部コマンド処理部２４は、アドレス情報管理領域５４にZZZZの値を保存し、あわせて、ZZZZの値に対応するようにセキュア領域と認証領域との論理ー物理アドレス変換テーブルを修正する。（ただし、（1’）の認証が行われ

ていない場合は境界アドレスの変更を拒否し、拒否したことをＩＣコマンド処理部１３に通知する）

（４）制御部コマンド処理部２４は、セキュア領域を拡張した場合に、新たにセキュア領域となった部分のデータを消去し、セキュア領域を縮小した場合に、新たに認証領域となった部分のデータを消去する。また、 セキュア領域、及び／または、認証領域のすべてのデータを消去してもよい。

（５）制御部コマンド処理部２４は、ＩＣコマンド処理部１３に境界変更完了を伝え、ＩＣコマンド処理部１３は、端末に境界変更完了を通知する（ただし、（３’）において境界アドレスの変更が拒否された場合は、端末に境界変更の拒否を通知する）。

また、認証領域の拡張／縮小は、認証領域と非認証領域との境界の第２アドレス情報を変更することにより行う。この場合の手順は次のようになる。

（１）端末は、セキュアメモリカード１０の制御部２０に対して認証を要求し、制御コマンド処理部２４の指示により、制御認証部２３が認証領域のサイズ変更を許可するための認証を行う。

（２）認証を受けた端末は、制御部２０に対して変更後の第２アドレス情報（新たなXXXX）を通知する。

（３）制御部コマンド処理部２４は、アドレス情報管理領域５４にXXXXの値を保存し、あわせて、XXXXの値に対応するように非認証領域と認証領域との論理ー物理アドレス変換テーブルを修正する（ただし、（１）の認証が行われていない場合は境界アドレスの変更を拒否し、拒否したことを端末に通知する）。

（４）制御部コマンド処理部２４は、認証領域を拡張した場合に、新たに認証領域となった部分のデータを消去し、認証領域を縮小した場合に、新たに非認証領域となった部分のデータを消去する。また、 非認証領域、及び／または、認証領域のすべてのデータを消去してもよい。

（５）制御部コマンド処理部２４は、端末に境界変更完了を通知する。

なお、この場合、図１０に示すように、論理ー物理アドレス変換テーブルの非認証領域５３における論理アドレスの順番が物理アドレスの順序の正順であり、認証領域５２における論理アドレスの順番が物理アドレスの順序の逆順であると、

境界変更の際に、ともに論理ブロックの末尾アドレスの側だけを修正すれば足りるので、境界変更に伴うテーブルの書き換え負担が少なくなり、高速での処理が可能になる。

非認証領域の拡張／縮小は、認証領域の拡張／縮小処理により実現できる。

また、大容量不揮発性メモリ５０には、図１１に示すように、セキュア領域５１、非認証領域５３、認証領域５２の順に各領域を配置しても良い。図１２には、このときの論理ー物理アドレス変換テーブルの一例を示している。

また、この場合、セキュア領域５１を端末から見えない領域とするため、または、セキュア領域を持たないメモリカードとの互換性を保つために、図１１に示すように、実際の境界アドレスとは異なる「端末みなしアドレス」を設けるようにしてもよい。この端末みなしアドレスでは、セキュア領域を省いて、非認証領域５３の先頭のみなし物理アドレスを 0000 とし（実際は XXXX'）、非認証領域５３と認証領域５２との境界のみなし物理アドレスを ZZZZ''（実際は ZZZZ'）、認証領域終端のみなし物理アドレスを YYYY''（実際は YYYY'）とする。端末は境界アドレスを ZZZZ'' と認識し、領域の拡張／縮小を要求する際に、この ZZZZ'' の変更を要求するが、制御コマンド処理部は、ZZZZ'' と ZZZZ' との関係を認識し、実際の物理アドレス ZZZZ' に置き換えて、境界の変更を行う。

なお、本発明の実施形態では、大容量不揮発性メモリ５０に、記憶領域として、非認証領域、認証領域及びセキュア領域の３領域を設ける場合について説明したが、大容量不揮発性メモリ５０に、セキュア領域の他に、非認証領域または認証領域の一方だけを通常領域として設けるようにしても良い。

また、ここでは主に、セキュアメモリカードのＩＣ部に決済用アプリケーションを搭載する場合について説明したが、その他、署名を生成するアプリケーションを搭載することも可能である。

この場合、データのセキュア領域への書き込み時に書き込みデータのハッシュ値を計算し、それをＩＣ部の内部不揮発性メモリに格納し、ハッシュ値に対して電子署名を生成する。データのセキュア領域からの読み出し時（復号化後）には、再度ハッシュ値を計算し、書き込み時にＩＣ部の内部不揮発性メモリに格納したハッシュ値と比較することでデータの欠損、改ざんなどを検知する。

こうした機能を搭載することで、このセキュアメモリカードは、決済する際に利用することもできるし、何らかのデータに電子署名を付与する際にも利用することができる。

また、このセキュアメモリカードを用いるＲ／Ｗ装置として、デジタルコンテンツ配信サービス用アプリケーションを搭載し、決済機能と、コンテンツのダウンロード及びメモリカードへの格納機能とを持つ場合について説明したが、セキュアメモリカードを活用する上で、Ｒ／Ｗ装置には次の機能を持つことが求められる。

・セキュアメモリカードの通常領域を読み書きするためのコマンドを生成することができる。

・セキュアメモリカードのＩＣ部に処理を要求するためのＩＣコマンドを生成することができる。

・ＩＣ部アプリケーション（ＩＣ認証部）と認証を行うための認証鍵を取得して、それを用いて認証に必要なデータ（ＩＣ部アプリケーションから提供された乱数に対して暗号または署名を施したデータ）を生成することができる。

また、セキュアメモリカードが通常領域として、非認証領域及び認証領域を有する場合には、これに加えて、

・認証領域を読み書きするためのコマンドを生成することができる。

・セキュアメモリカードの制御認証部と認証を行うための認証鍵を取得して、それを用いて認証に必要なデータを生成することができる。

ことが求められる。

なお、認証鍵の取得は、Ｒ／Ｗ装置（電子機器）が認証鍵をＲＯＭなどで保持している場合には、そこから入手する。また、電子機器が認証鍵を保持していない場合には、外部の機器（サーバ、リムーバブルメディア等）から受信する。

また、本発明のセキュアメモリカード１０が有する大容量不揮発性メモリ５０を、他の記憶メディア、例えば、ハードディスク、光ディスク、光磁気ディスク等の不揮発メディアに置き換えても、本発明と同様、大容量・高セキュリティなメモリデバイスが実現されることは言うまでもない。

また、本発明のセキュアメモリカード１０は、電子機器に対して着脱可能である必要は無く、例えば電子機器にＩＣチップを埋め込んだ一体型機器などのように、電子機器と固定的に接続されていても良い。また、カード／チップのような形状である必要もなく、ディスクやテープなどの形態であっても一向に構わない。

また、本発明の電子機器（６０、６１、６９）は、固定設置端末、携帯端末、携帯電話など、メモリデバイスが接続できるものであればどのようなものでも一向に構わない。

つまり、本発明の実施形態で説明したもの以外でも、携帯電話にＩＣチップを埋め込んだもの、固定設置端末にハードディスクを装着したようなもの等、その用途に応じて様々な形態が考えられる。

本発明を詳細に、また、特定の実施態様を参照して説明したが、本発明の精神と範囲を逸脱することなく、様々な変更や修正を加えることができることは、当業者にとって明らかである。

本出願は、２００２年１２月１６日出願の日本特許出願（特願２００２－３６３５９７号）に基づくものであり、その内容は、ここに参照して取り込まれる。

＜産業上の利用可能性＞

以上の説明から明らかなように、本発明のメモリデバイスは、セキュリティレベルがＩＣカードと同等であって、記憶容量がＩＣカードに比べて遥かに大きいメモリ領域を持つことができる。

また、このメモリデバイスは、複数のセキュリティレベルのメモリ領域を備えており、一つのデバイスでデジタルキャッシュや音楽配信等の多用なサービスに対応することができる。また、この複数のメモリ領域の大きさは、必要に応じて変更することができる。

また、本発明の電子機器（Ｒ／Ｗ装置）は、このメモリデバイスを活用して、多様なサービスの実現を図ることができる。

請求の範囲

1. 電子機器に固定的にまたは着脱可能に接続されるメモリデバイスであって、

前記電子機器からアクセスすることが可能な通常領域と、前記電子機器から直接アクセスすることができないセキュア領域とを有する、非耐タンパー性の第１のメモリと、

前記電子機器から直接アクセスすることができない耐タンパー性の第２のメモリと、

前記第２のメモリへのアクセスを管理するセキュア制御部と、

を備えており、

前記電子機器から前記第１のメモリのセキュア領域へのアクセスは、前記セキュア制御部を介してのみ可能であること、

を特徴とするメモリデバイス。

2. 請求項１に記載のメモリデバイスであって、

前記セキュア制御部は、前記セキュア制御部が認証した電子機器のコマンドを受けて前記セキュア領域または第２のメモリにアクセスし、データの書き込みまたは読み出しを行うこと、

を特徴とするメモリデバイス。

3. 請求項１または請求項２に記載のメモリデバイスであって、

前記第２のメモリには、暗号鍵が格納されており、

前記セキュア制御部は、前記セキュア領域に書き込むデータを前記暗号鍵を用いて暗号化して書き込み、且つ、前記セキュア領域から読み出したデータを前記暗号鍵を用いて復号化すること、

を特徴とするメモリデバイス。

4 請求項１から請求項３のいずれかに記載のメモリデバイスであって、

前記セキュア制御部は、前記セキュア領域に書き込むデータのハッシュ値を計算して、前記ハッシュ値を前記第２のメモリに格納し、前記セキュア領域から読み出したデータのハッシュ値を計算して、前記第２のメモリに格納したハッシュ値と照合すること、

を特徴とするメモリデバイス。

５　請求項１に記載のメモリデバイスであって、

前記第１のメモリの通常領域が、メモリデバイスを制御する全体制御部によって認証された電子機器のみがアクセスできる認証領域と、認証を受けない電子機器でもアクセスできる非認証領域とを含むこと、

を特徴とするメモリデバイス。

６　請求項１から請求項５のいずれかに記載のメモリデバイスであって、

前記通常領域と前記セキュア領域との境界を示す境界アドレス情報と、前記通常領域及びセキュア領域の各々における論理アドレスと物理アドレスとの関係を記述した論理－物理アドレス変換テーブルとが、前記第１のメモリのアドレス情報として管理されていること、

を特徴とするメモリデバイス。

７．　請求項６に記載のメモリデバイスであって、

前記第１のメモリのアドレス情報に、前記認証領域と前記非認証領域との境界を示す境界アドレス情報と、前記認証領域及び非認証領域の各々における論理－物理アドレス変換テーブルとが含まれていること、

を特徴とするメモリデバイス。

８．　請求項６または請求項７に記載のメモリデバイスであって、

前記境界アドレス情報及び論理－物理アドレス変換テーブルが、前記第１のメモリのアドレス情報管理領域に記録されていること、

を特徴とするメモリデバイス。

９　　請求項６に記載のメモリデバイスであって、

前記境界アドレス情報で表された前記通常領域と前記セキュア領域との境界が、前記セキュア制御部の認証を受けた電子機器のコマンドで変更されること、

を特徴とするメモリデバイス。

１０　　請求項７に記載のメモリデバイスであって、

前記境界アドレス情報で表された前記認証領域と前記非認証領域との境界が、前記全体制御部の認証を受けた電子機器のコマンドで変更されること、

を特徴とするメモリデバイス。

１１　　請求項１０に記載のメモリデバイスであって、

前記認証領域と前記非認証領域との境界の境界アドレス情報が、実境界アドレスと、セキュア領域を除いて設定したみなし境界アドレスとから成り、

前記全体制御部の認証を受けた電子機器のコマンドによって指定された前記みなし境界アドレスに基づいて、前記実境界アドレスが変更されること、

を特徴とするメモリデバイス。

１２　　メモリ領域として第１領域、第２領域、及び第３領域を有するメモリデバイスに対して、アクセスを行う電子機器であって、

前記電子機器は、メモリデバイスへのアクセス要求を受けると、

メモリデバイスの非耐タンパー性のメモリ領域である前記第１領域に、メモリデバイスへのアクセスを制御するメモリデバイスの全体制御部を介してアクセスし、

前記全体制御部、並びに、第２領域及び第３領域へのアクセスを制御するメモリデバイスのセキュア制御部の認証を受けた後、第１領域以外の非耐タンパー性のメモリ領域である前記第２領域には、前記セキュア制御部を介してアクセスし、

前記セキュア制御部との認証を経た後、メモリデバイスの耐タンパー性のメモリ領域である前記第３領域には、前記全体制御部及び前記セキュア制御部を介してアクセスする、

ことを特徴とする電子機器。

１３．　請求項１２に記載の電子機器であって、

第１領域に対するデータの書き込みまたは読み出しのコマンドを生成する第１のコマンド生成手段と、

セキュア制御部に処理を要求するコマンドを生成する第２のコマンド生成手段と、

前記セキュア制御部との認証に用いる認証鍵を取得し、前記セキュア制御部との認証処理を行う第１の認証処理手段と、

を備える電子機器。

１４．　請求項１２または請求項１３に記載の電子機器であって、

第１領域の一部の領域である非認証領域には、全体制御部との認証を経ることなくアクセスを行い、非認証領域以外で、第１領域の一部または全部の領域である認証領域には、全体制御部との認証を経た後にアクセスを行う、

ことを特徴とする電子機器。

１５．　請求項１４に記載の電子機器であって、

認証領域に対するデータの書き込みまたは読み出しのコマンドを生成する第３のコマンド生成手段と、

全体制御部との認証に用いる認証鍵を取得し、前記全体制御部との認証処理を行う第２の認証処理手段と、

を備える電子機器。

図 1

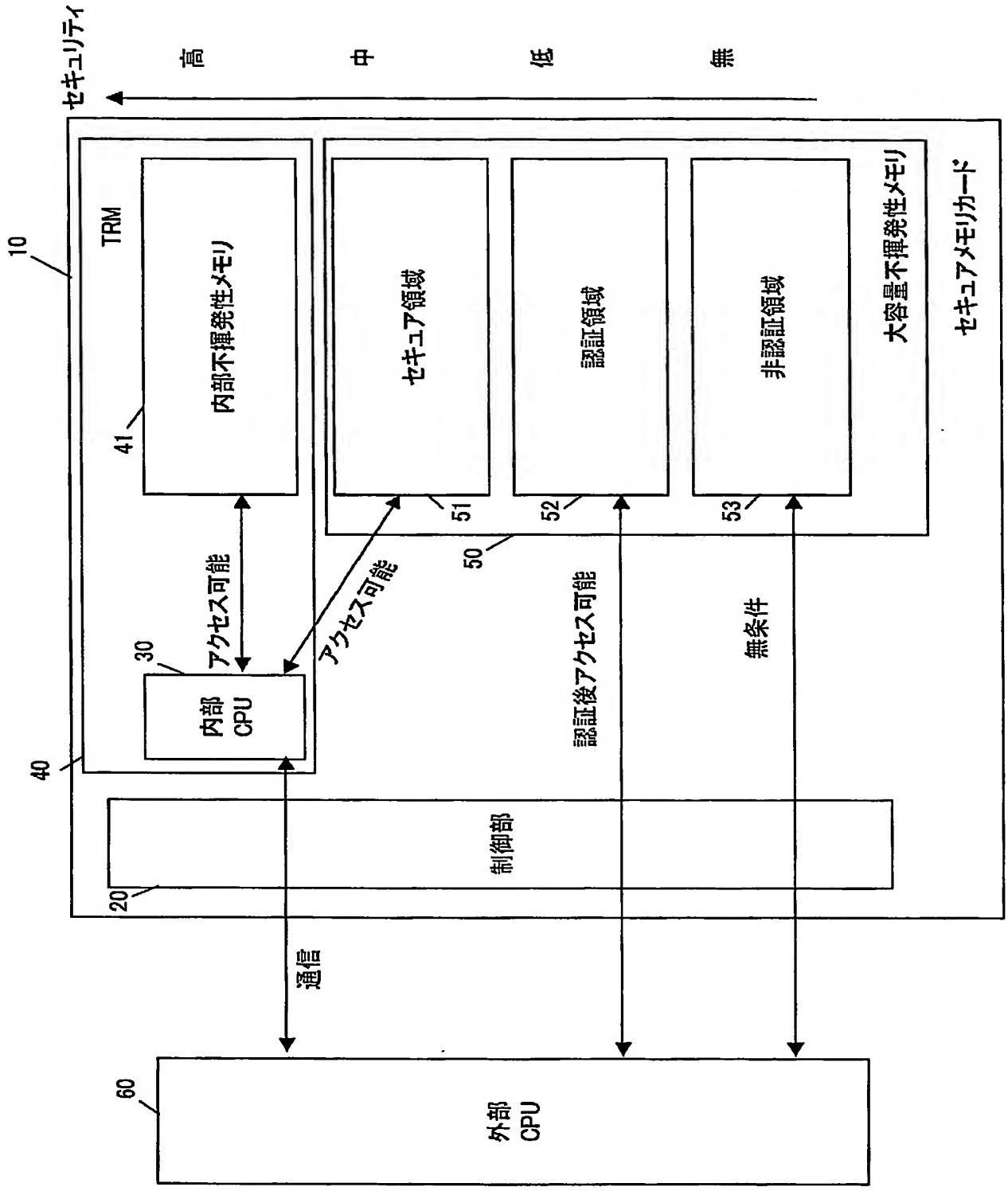

セキュリティ
高
中
低
無
10
TRM
内部不揮発性メモリ
41
セキュア領域
51
認証領域
52
非認証領域
53
大容量不揮発性メモリ
セキュアメモリカード
50
アクセス可能
30
内部 CPU
アクセス可能
認証後アクセス可能
無条件
40
制御部
20
通信
60
外部 CPU

図 2

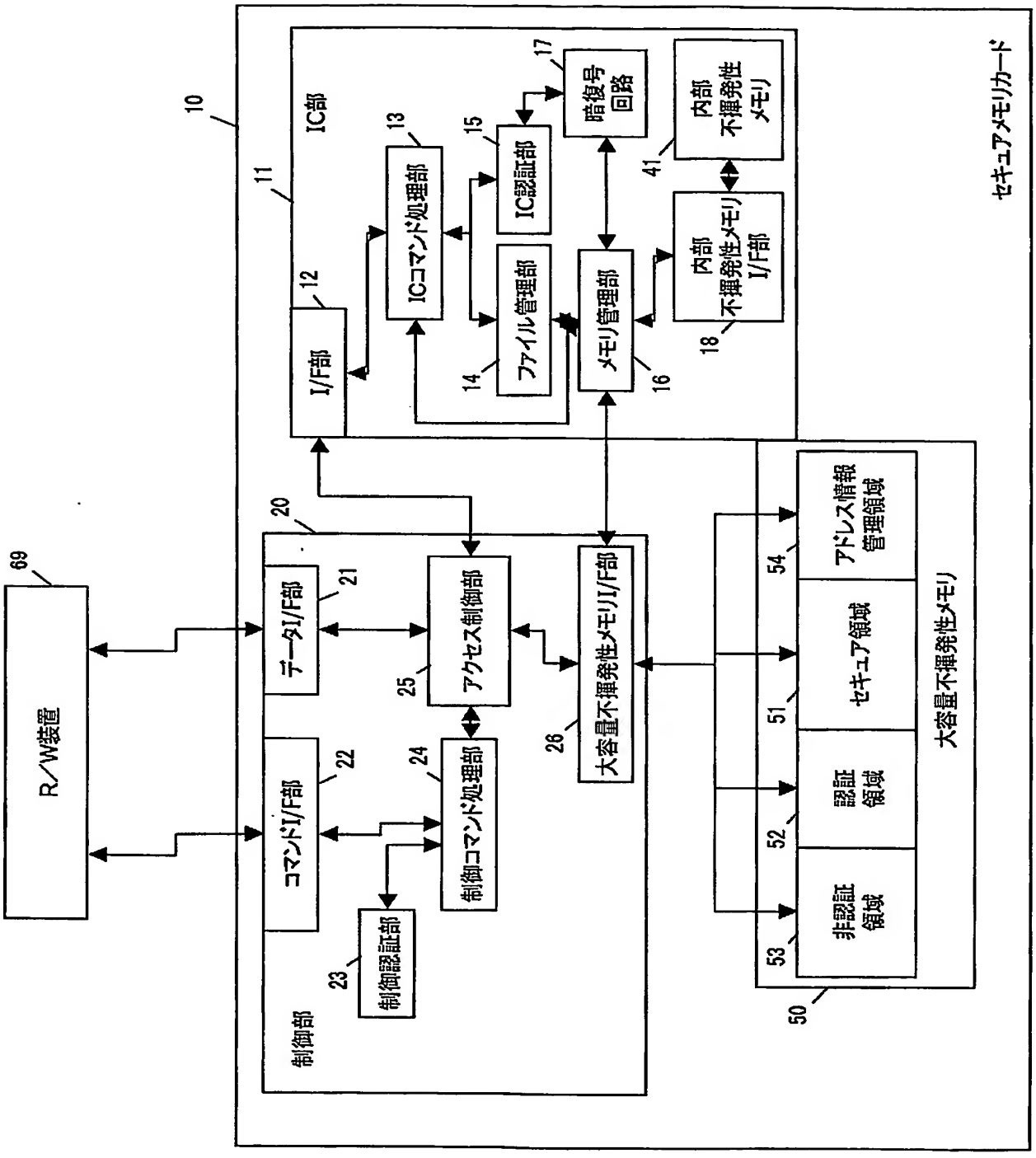

セキュアメモリカード
10
IC部
11
I/F部
12
ICコマンド処理部
13
IC認証部
15
暗復号回路
17
ファイル管理部
14
メモリ管理部
16
内部不揮発性メモリI/F部
18
内部不揮発性メモリ
41
制御部
20
データI/F部
21
コマンドI/F部
22
制御認証部
23
制御コマンド処理部
24
アクセス制御部
25
大容量不揮発性メモリI/F部
26
R/W装置
69
大容量不揮発性メモリ
50
非認証領域
53
認証領域
52
セキュア領域
51
アドレス情報管理領域
54

図３

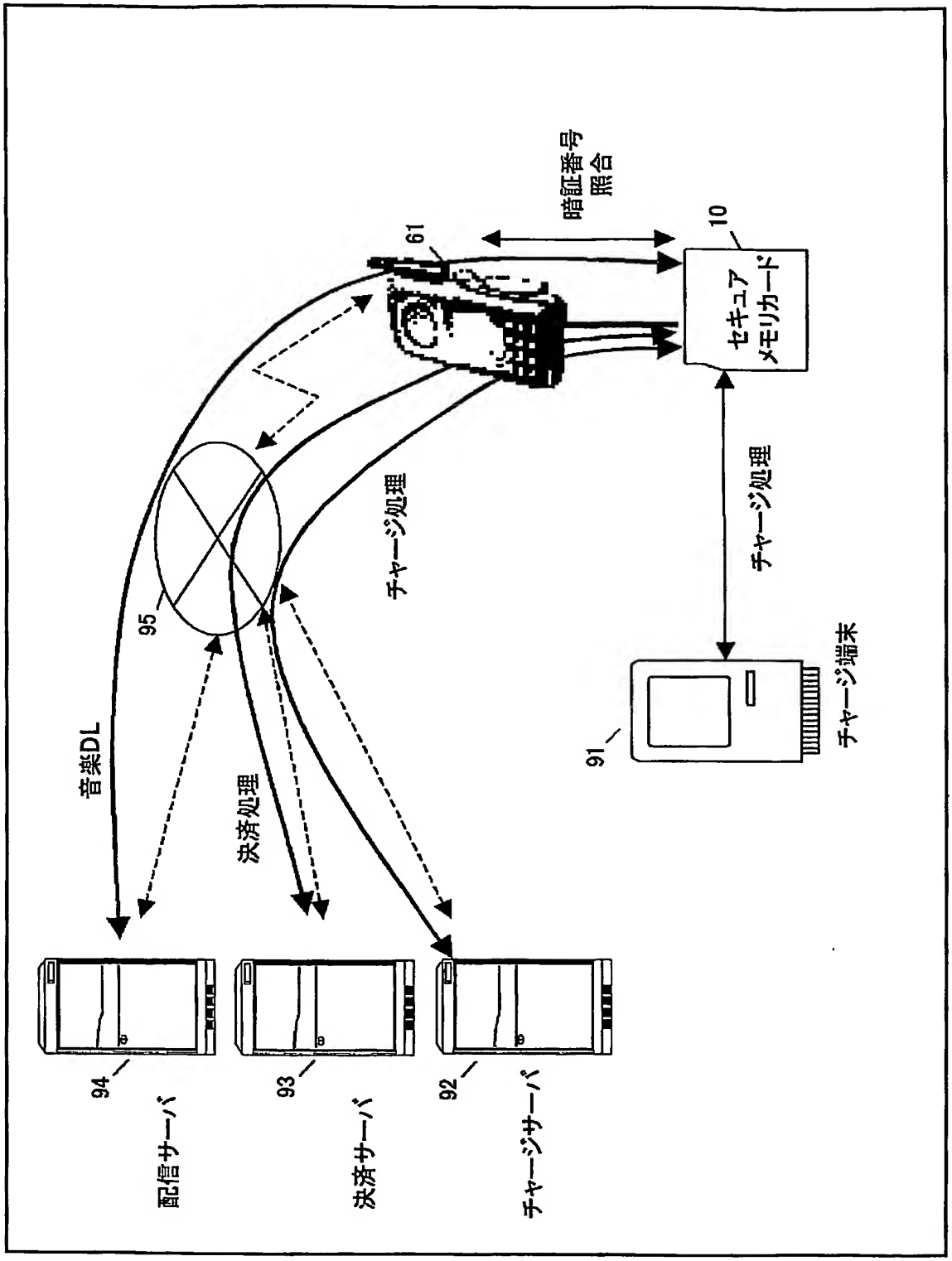

暗証番号照合
61
10
セキュアメモリカード
チャージ処理
チャージ処理
95
音楽DL
決済処理
91
チャージ端末
94
配信サーバ
93
決済サーバ
92
チャージサーバ

図４

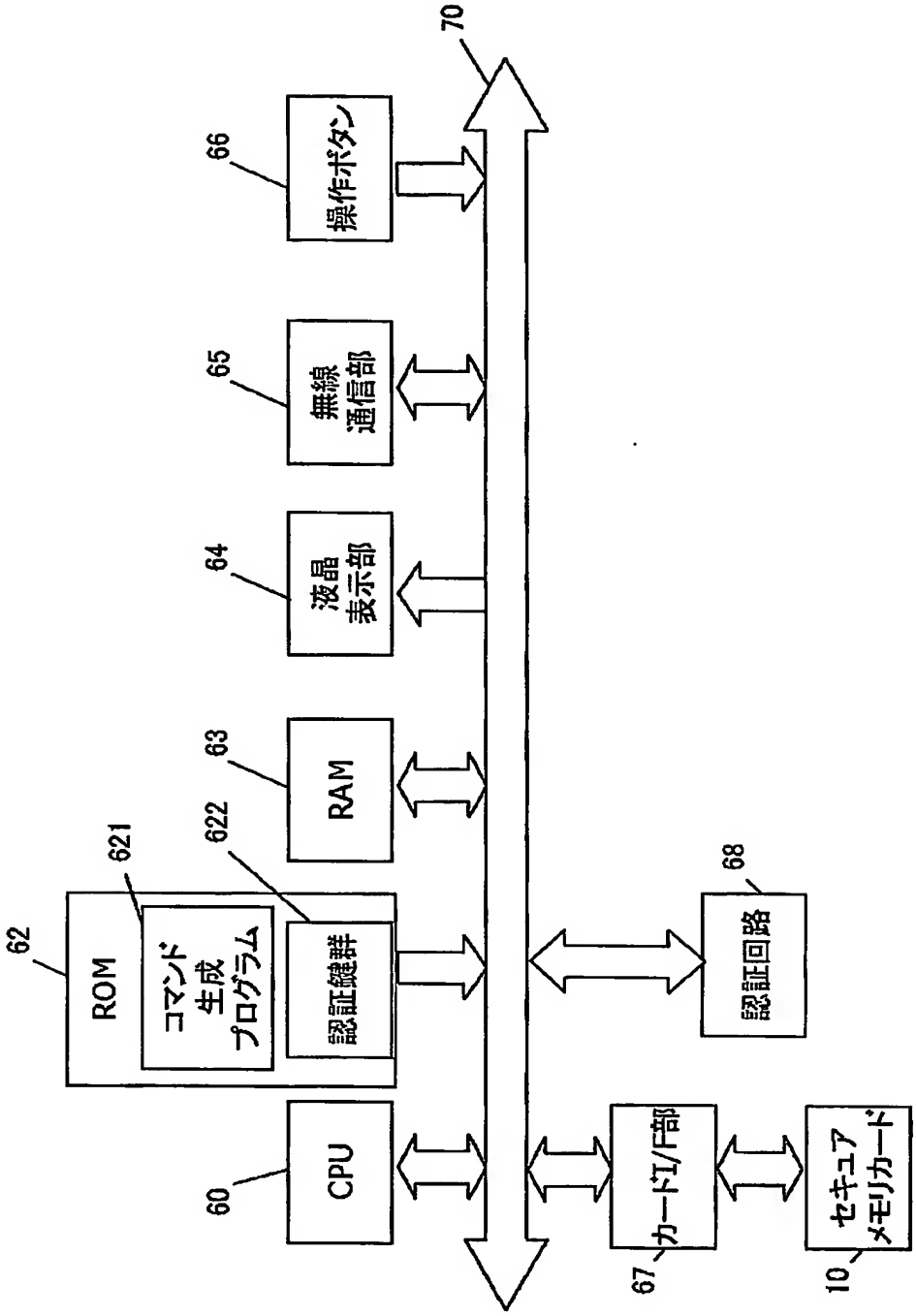

70
66
操作ボタン
65
無線通信部
64
液晶表示部
63
RAM
62
ROM
621
コマンド生成プログラム
622
認証鍵群
68
認証回路
60
CPU
67
カードI/F部
10
セキュアメモリカード

図 5

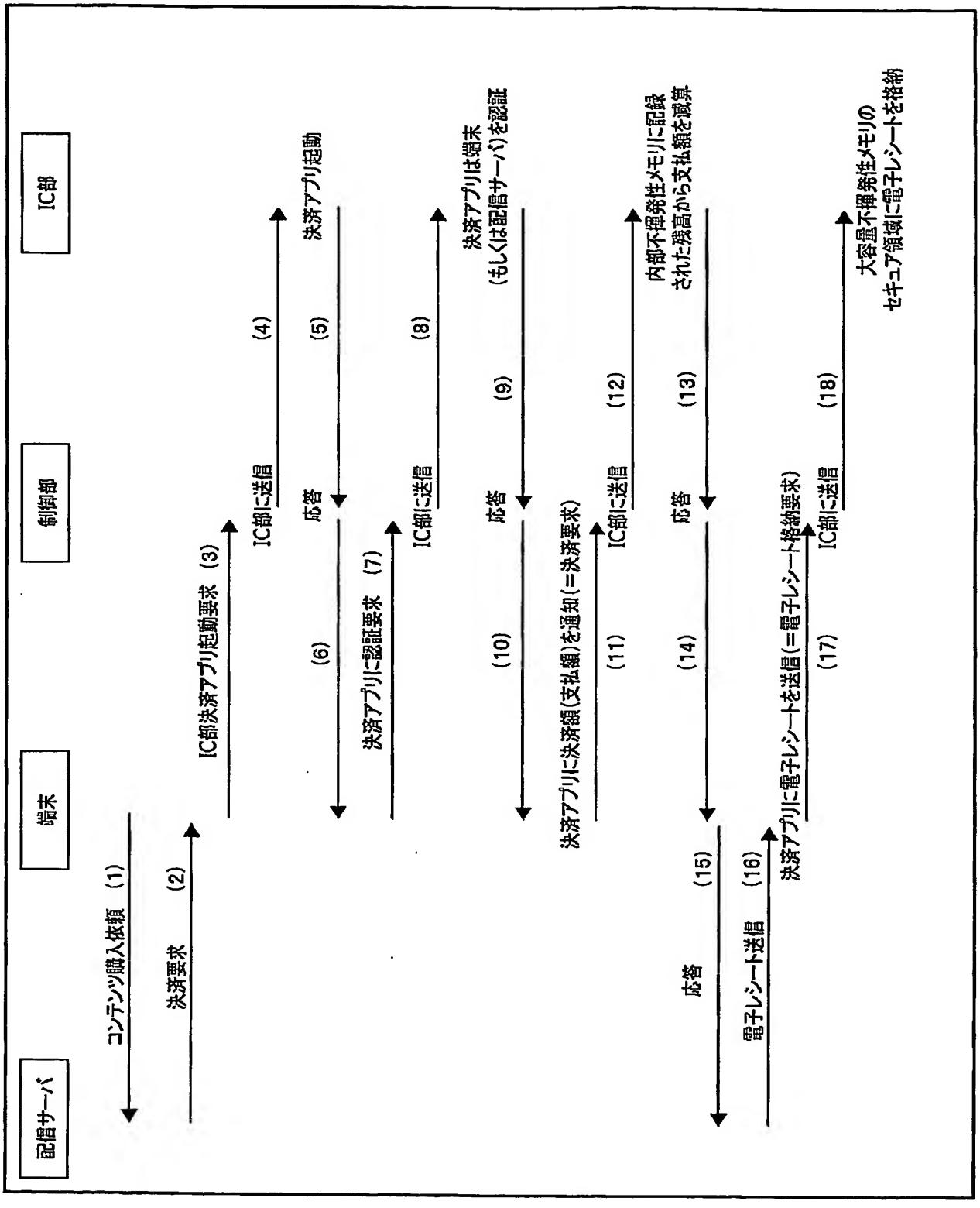

配信サーバ
端末
制御部
IC部
コンテンツ購入依頼 (1)
決済要求 (2)
IC部決済アプリ起動要求 (3)
IC部に送信 (4)
決済アプリ起動
応答 (5)
(6)
決済アプリに認証要求 (7)
IC部に送信 (8)
決済アプリは端末
(もしくは配信サーバ)を認証
応答 (9)
(10)
決済アプリに決済額(支払額)を通知(=決済要求)
IC部に送信 (11)
(12)
内部不揮発性メモリに記録
された残高から支払額を減算
応答 (13)
(14)
応答 (15)
電子レシート送信 (16)
決済アプリに電子レシートを送信(=電子レシート格納要求)
IC部に送信 (17)
(18)
大容量不揮発性メモリの
セキュア領域に電子レシートを格納

図 6

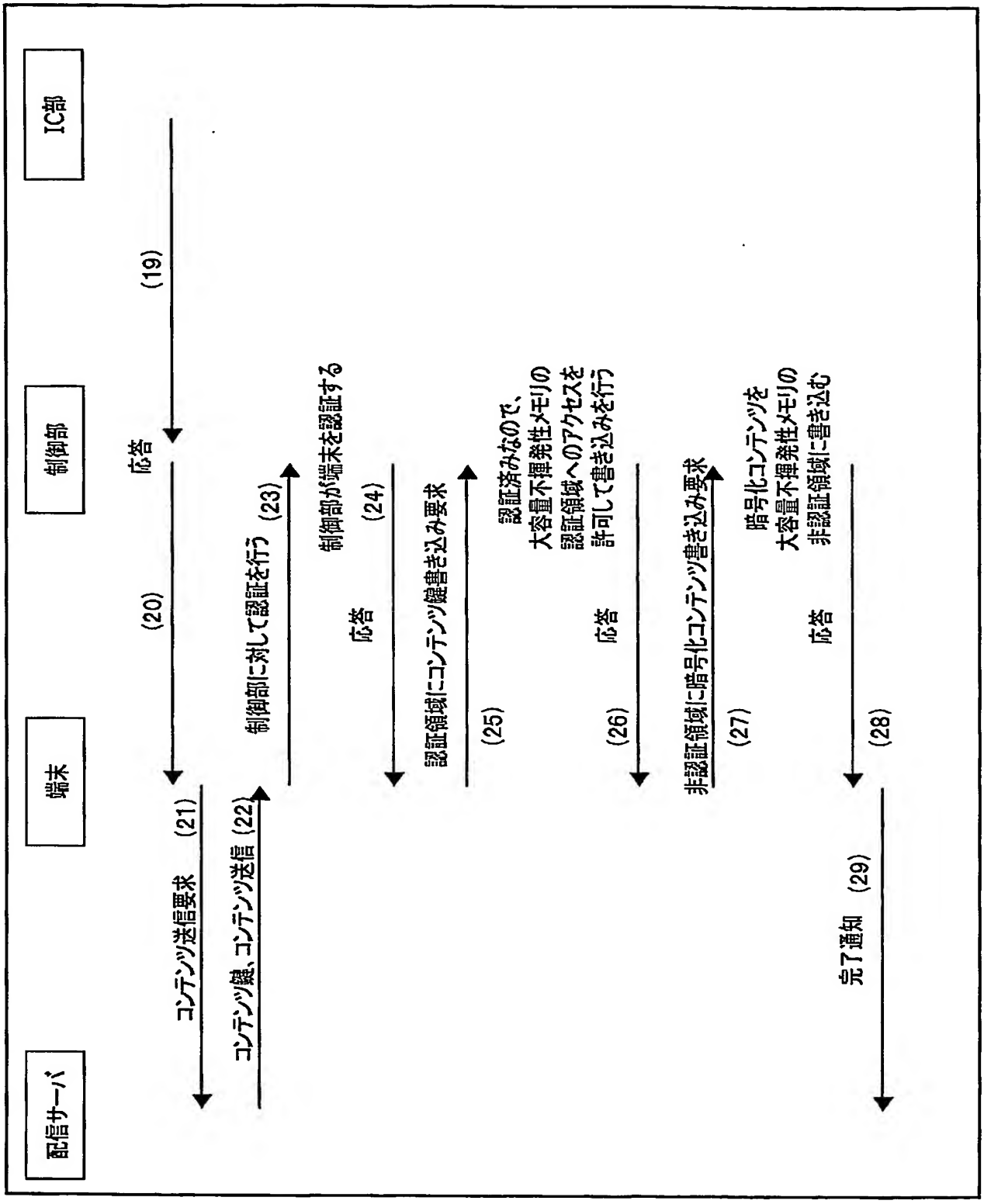

配信サーバ
端末
制御部
IC部
(19)
応答
(20)
コンテンツ送信要求 (21)
コンテンツ鍵、コンテンツ送信 (22)
制御部に対して認証を行う (23)
制御部が端末を認証する
応答 (24)
認証領域にコンテンツ鍵書き込み要求
(25)
認証済みなので、
大容量不揮発性メモリの
認証領域へのアクセスを
許可して書き込みを行う
応答 (26)
非認証領域に暗号化コンテンツ書き込み要求
(27)
暗号化コンテンツを
大容量不揮発性メモリの
非認証領域に書き込む
応答 (28)
完了通知 (29)

図 7

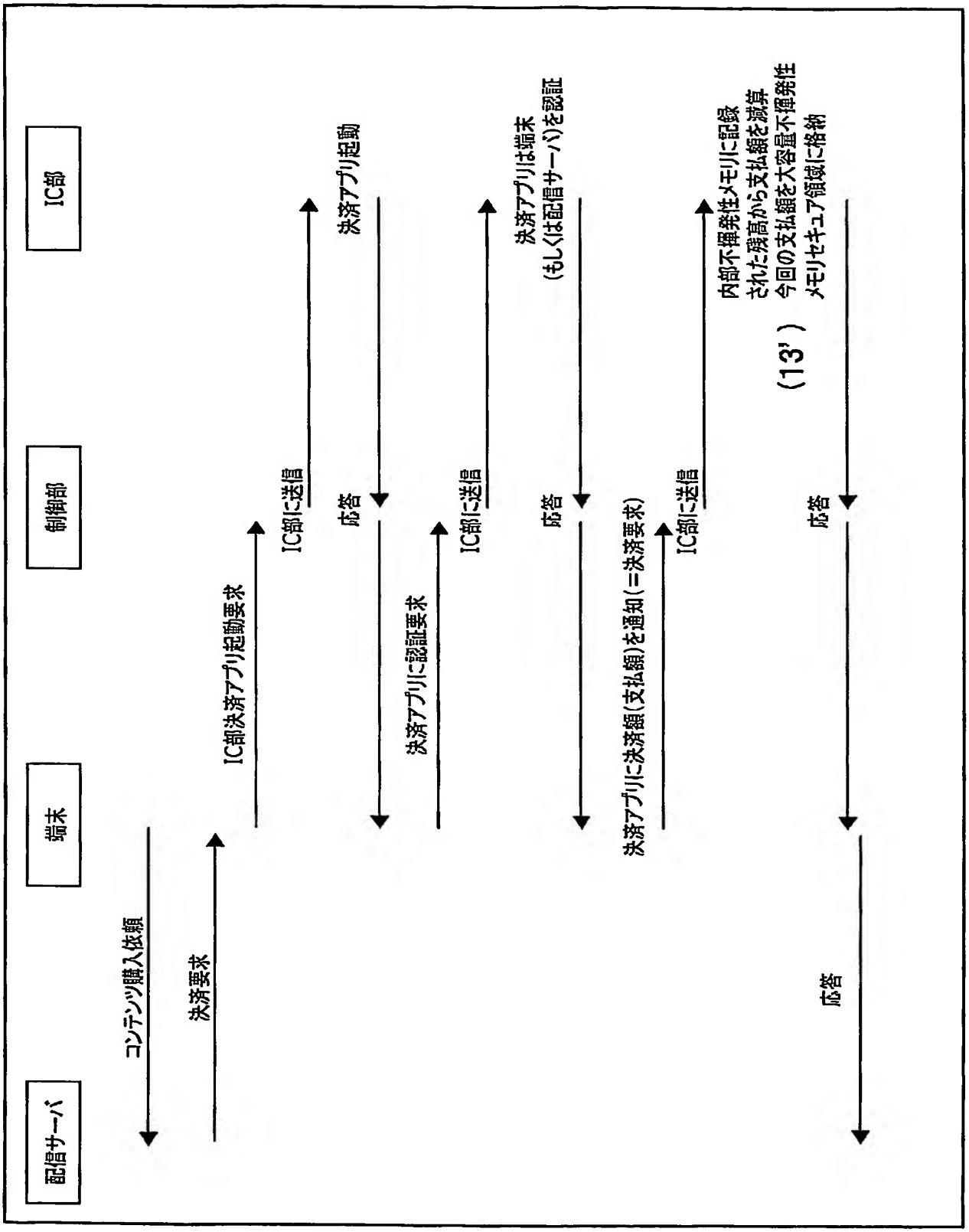

配信サーバ
端末
制御部
IC部
コンテンツ購入依頼
決済要求
IC部決済アプリ起動要求
IC部に送信
決済アプリ起動
応答
決済アプリに認証要求
IC部に送信
決済アプリは端末
(もしくは配信サーバ)を認証
応答
決済アプリに決済額(支払額)を通知(=決済要求)
IC部に送信
内部不揮発性メモリに記録
された残高から支払額を減算
今回の支払額を大容量不揮発性
メモリセキュア領域に格納
(13')
応答
応答

図８

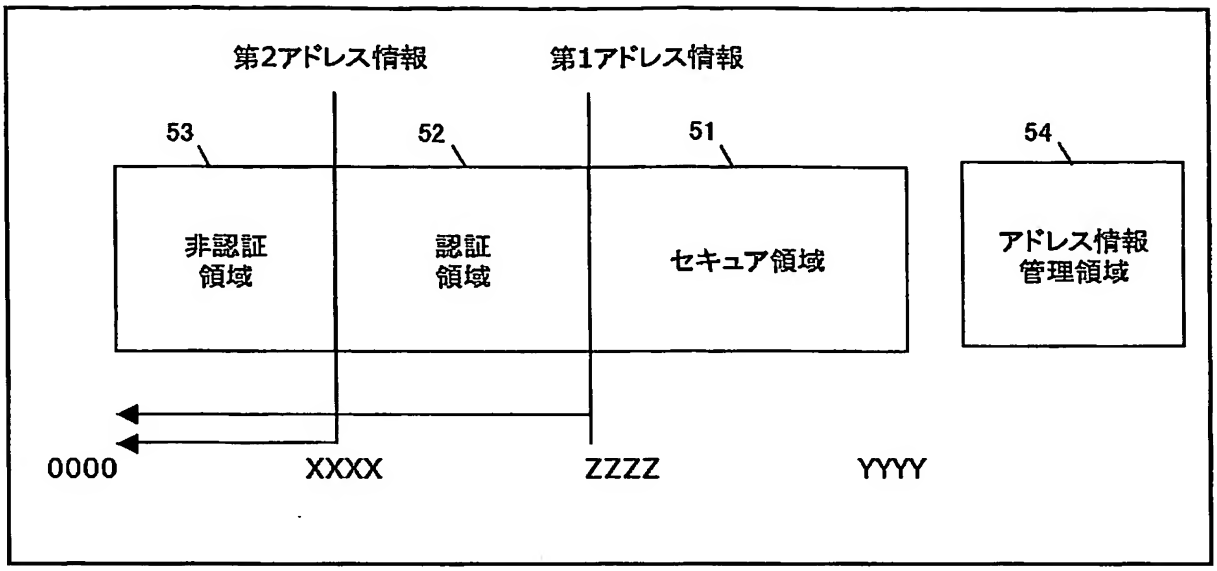

第2アドレス情報
第1アドレス情報
53
52
51
54
非認証
領域
認証
領域
セキュア領域
アドレス情報
管理領域
0000
XXXX
ZZZZ
YYYY

図 9

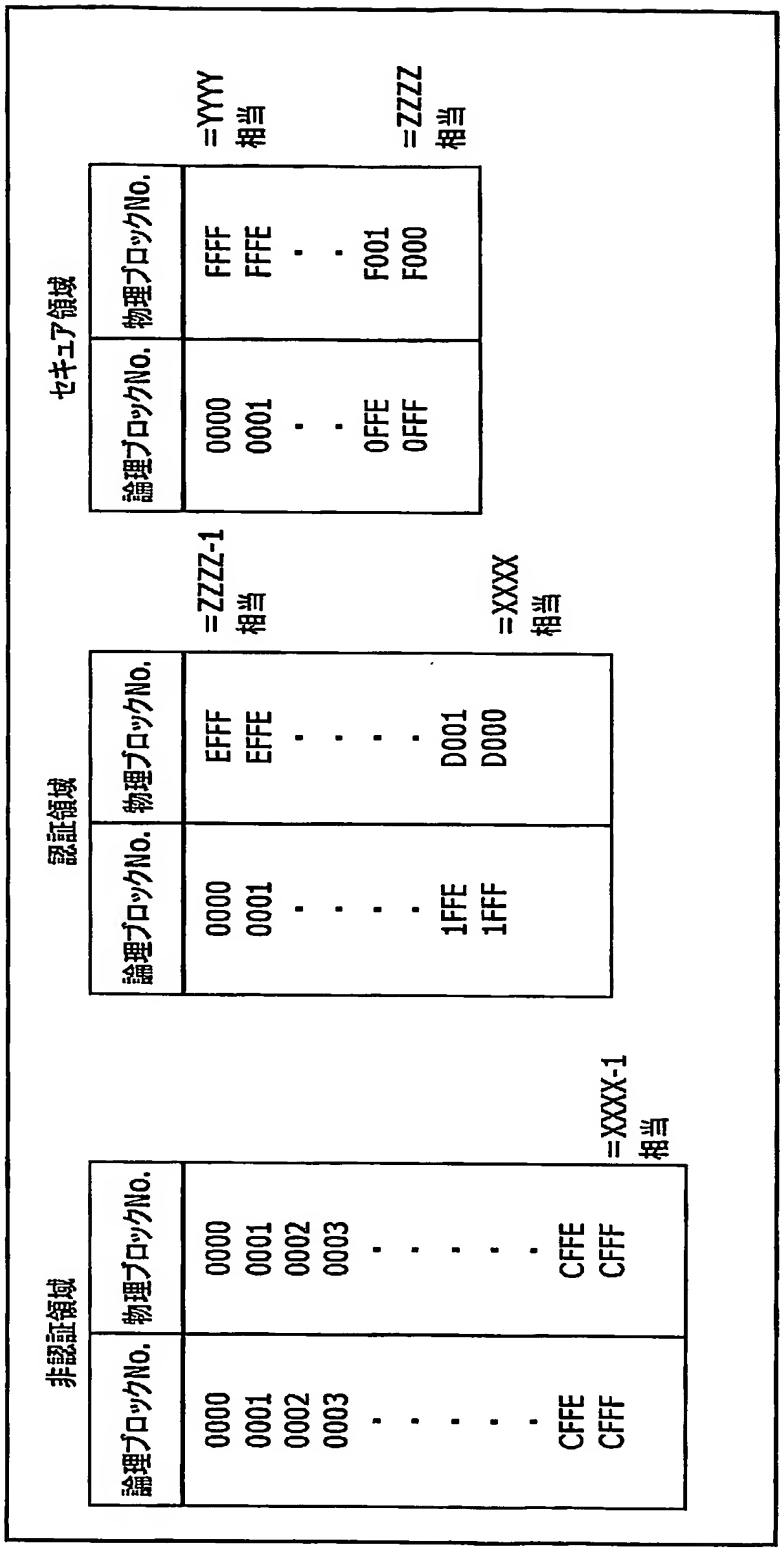

非認証領域
論理ブロックNo.
物理ブロックNo.
0000 0000
0001 0001
0002 0002
0003 0003
CFFE CFFE
CFFF CFFF
=XXXX-1 相当
認証領域
論理ブロックNo.
物理ブロックNo.
0000 EFFF
0001 EFFE
1FFE D001
1FFF D000
=ZZZZ-1 相当
=XXXX 相当
セキュア領域
論理ブロックNo.
物理ブロックNo.
0000 FFFF
0001 FFFE
0FFE F001
0FFF F000
=YYYY 相当
=ZZZZ 相当

図１０

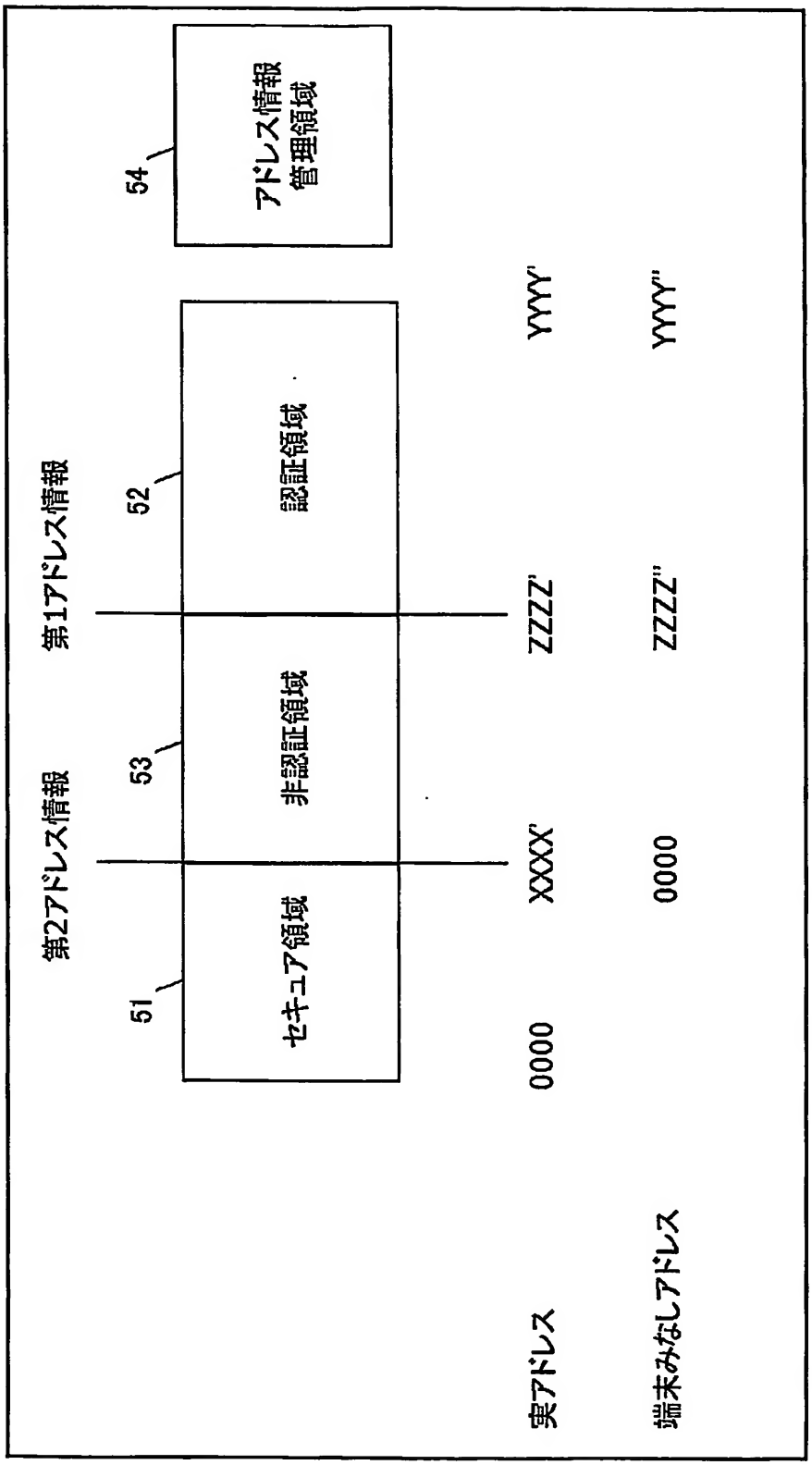

第2アドレス情報
第1アドレス情報
51
53
52
54
セキュア領域
非認証領域
認証領域
アドレス情報
管理領域
実アドレス
0000
XXXX'
ZZZZ'
YYYY'
端末みなしアドレス
0000
ZZZZ''
YYYY''

図１１

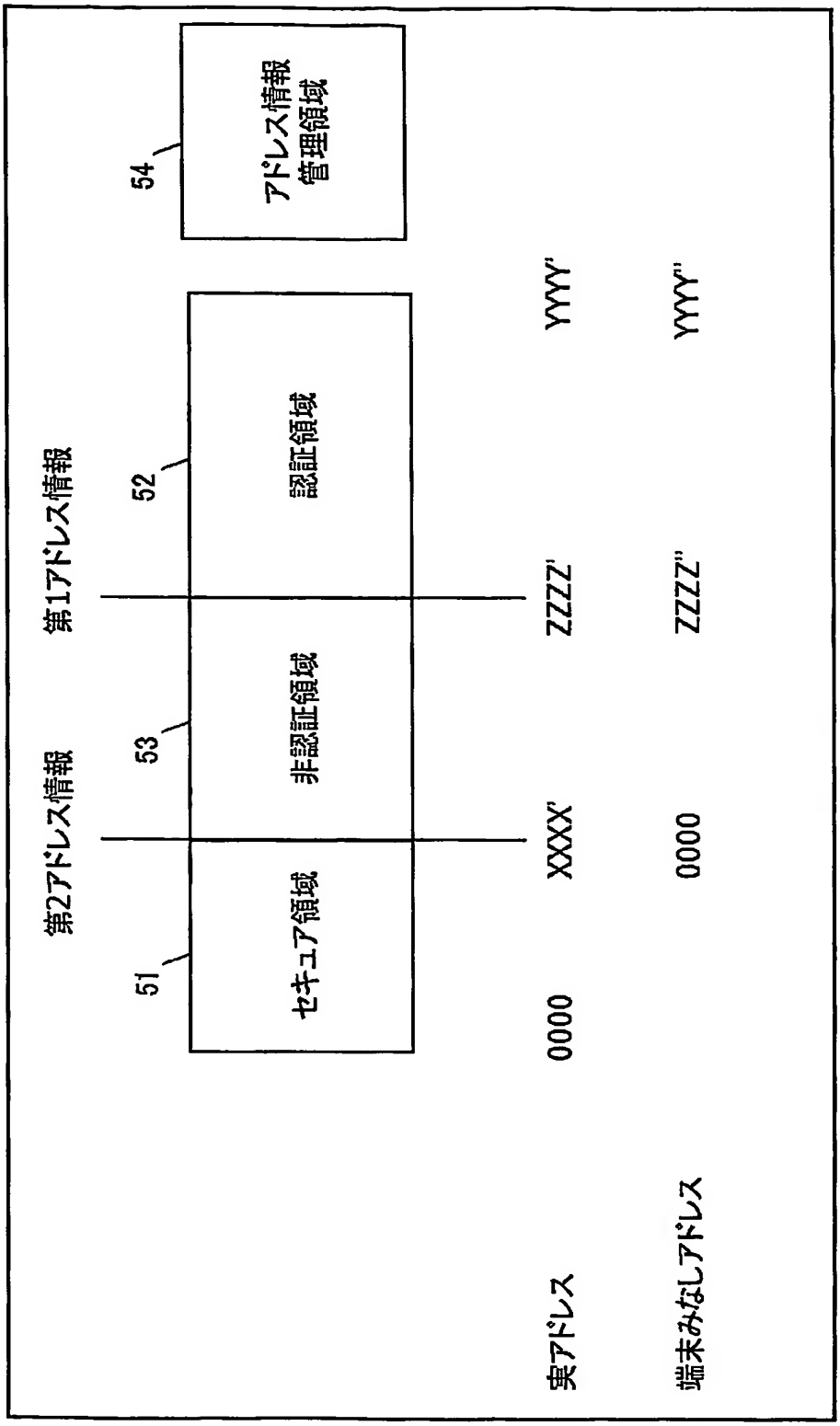
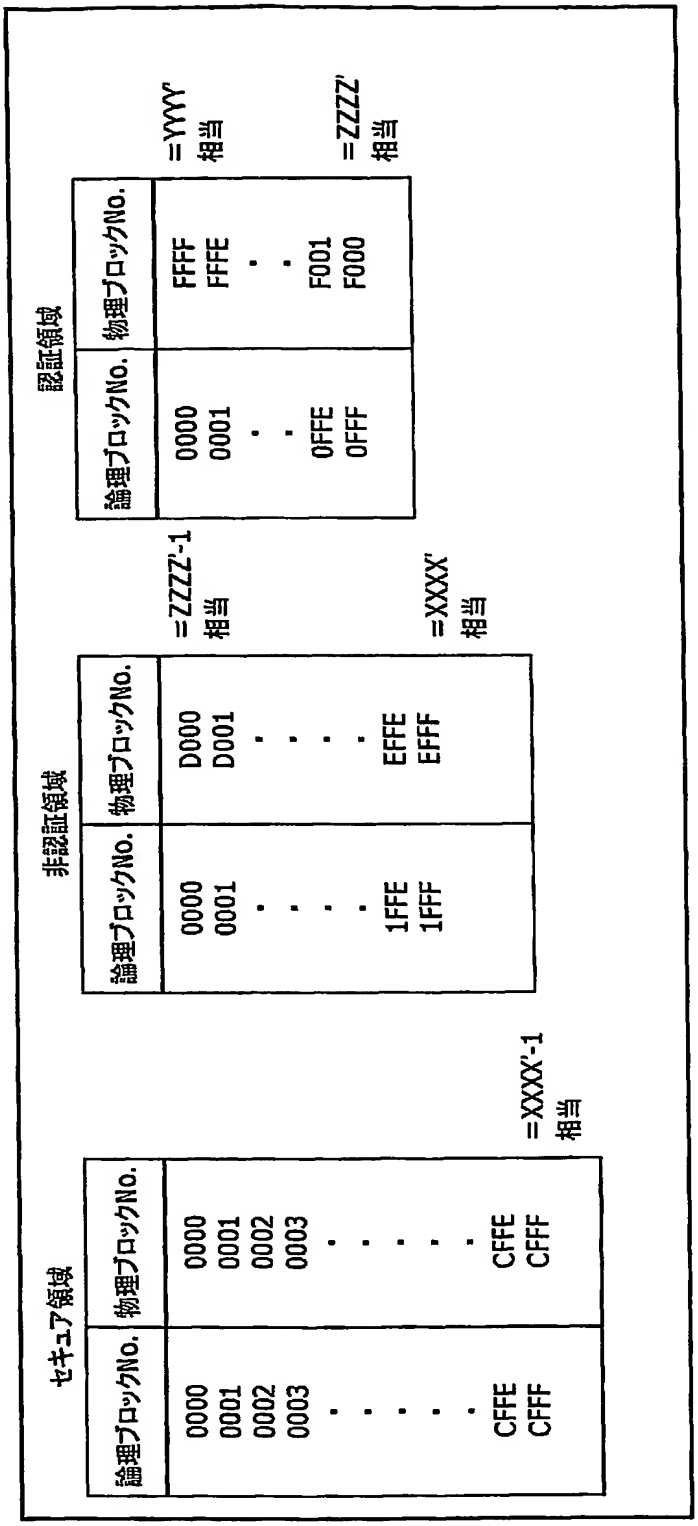

第2アドレス情報
第1アドレス情報
51
53
52
54
セキュア領域
非認証領域
認証領域
アドレス情報
管理領域
実アドレス
0000
XXXX'
ZZZZ'
YYYY'
端末みなしアドレス
0000
ZZZZ''
YYYY''

図１２


セキュア領域
論理ブロックNo.
物理ブロックNo.
0000 0000
0001 0001
0002 0002
0003 0003
CFFE CFFE
CFFF CFFF
=XXXX'-1 相当
非認証領域
論理ブロックNo.
物理ブロックNo.
0000 D000
0001 D001
1FFE EFFE
1FFF EFFF
=ZZZZ'-1 相当
=XXXX' 相当
認証領域
論理ブロックNo.
物理ブロックNo.
0000 FFFF
0001 FFFE
0FFE F001
0FFF F000
=YYYY' 相当
=ZZZZ' 相当

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/16000

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06K19/073

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-229861 A (Hitachi, Ltd.), 16 August, 2002 (16.08.02), Full text; all drawings & US 2002/169960 A1 & KR 2002065855 A	1-4,12-15 5-11
Y	JP 2001-14441 A (Matsushita Electric Industrial Co., Ltd.), 19 January, 2001 (19.01.01), Full text; all drawings & EP 1050887 A1 & EP 1050887 B1 & JP 3389186 B2 & JP 2003-233795 A & WO 2000/65602 A1 & AU 200036750 A & CN 1316087 A & KR 2001083073 A & BR 200007581 A	5-11

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 March, 2004 (10.03.04)	23 March, 2004 (23.03.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

国際調査報告

国際出願番号　PCT／JP03／16000

A.　発明の属する分野の分類（国際特許分類（IPC））
Int.Cl.[7]　G06F　12／14，G06K　19／073

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int.Cl.[7]　G06F　12／14，G06K　19／073

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　1922－1996年
日本国公開実用新案公報　　1971－2004年
日本国登録実用新案公報　　1994－2004年
日本国実用新案登録公報　　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	JP 2002-229861 A(株式会社日立製作所) 2002.08.16,全文,全図 & US 2002/169960 A1　& KR 2002065855 A	1-4,12-15 5-11
Y	JP 2001-14441 A(松下電器産業株式会社) 2001.01.19,全文,全図 & EP 1050887 A1　& EP 1050887 B1　& JP 3389186 B2 & JP 2003-233795 A　& WO 2000/65602 A1　& AU 200036750 A & CN 1316087 A　& KR 2001083073 A　& BR 200007581 A	5-11

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　10．03．2004

国際調査報告の発送日　23.3.2004

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号100－8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）　5N　2945
桜井　茂行

電話番号　03－3581－1101　内線　3545